CENTER FOR INFORMATION SYSTEMS SECURITY STUDIES AND RESEARCH

Assistant Professor Cynthia Irvine, Center Director
Department of Computer Science

The security of networked systems of computers is essential for national security. The Naval Postgraduate School is fortunate to be the home to what many researchers in the computer and network security community consider to be the preeminent program in the United States combining research and studies in information systems security (INFOSEC) and information assurance (IA). Since its inception, the Naval Postgraduate School Center for Information Systems Security Studies and Research (NPS CISR) has fostered an environment in which faculty, staff, and students work together to understand the information assurance requirements of DoD and to address the challenges presented by those requirements through careful analysis and research.

The need for focussed effort in information security and assurance is evident. The development of military strategy and tactics for warfare in the information age is of growing importance and has, as its principal objective, information superiority for U.S. forces engaged in battle on land, at sea or in the air. A key aspect of achieving information superiority is the protection of critical national information assets. Increasingly, military systems are dependent upon the national infrastructure for critical services. Today the United States faces an enormous problem. All aspects of the national infrastructure, from telecommunications to health care and from air traffic control to power systems, depend upon the correct operation of computers and networks. The security of those networks is crucial to the health of that infrastructure, yet security is often ignored as a fundamental requirement. Providing adequate protection for these information assets is a concern for the U.S. military and presents many new scientific and technical challenges in the area of INFOSEC and IA.

The October 1997 report of the Presidential Commission on Critical Infrastructure Protection (PCCIP) recommends, "*education on methods of reducing vulnerabilities and responding to attacks on critical infrastructures, …programs for curriculum development at the undergraduate and graduate levels in resilient system design practices,*" and efforts to make the "*required skill set much broader and deeper in educational level [for] computer scientists, network engineers, electronics engineers, [and] business process engineers.*"

Anticipating these recommendations by more than five years, NPS, with support from the National Security Agency (NSA), initiated a modest effort within the Computer Science Department to build a prototype program with three objectives: the development of courses on computer and network security based in a strong curriculum of science and engineering; research in information system security; and development of a cadre of officer-graduates with a thorough understanding of computer and network security

-- continued on page 5

About the DIRECTOR

Cynthia Irvine is an Assistant Professor in the Department of Computer Science. Prior to joining the faculty at NPS in 1994, she worked at Gemini Computers on several projects to utilize Class A1 technology for applications ranging from file systems to messaging prototypes. She received her undergraduate and Ph.D. degrees from Rice University and Case Western Reserve University, respectively. She has participated in the development and review of several interpretations of and guidelines for the Trusted Computer System Evaluation Criteria and has provided critical comments on emerging standards for the evaluation of trusted systems. Her current research and teaching interests are in the area of network security architectures and high assurance multilevel distributed systems.

CISR, *continued from page 4*

Center Director, Cynthia Irvine, joins students, LT Susan Bryer Joyner, LT Scott Heller and Capt Jason Hackerson, in the Computer Security Lab.

issues. An essential notion behind the development of NPS CISR is that the security of information systems must be founded on scientific and engineering principles which are used to construct secure systems rather than to discover after deployment that systems are inadequate.

Within a few years, the success of these early efforts was clear. Hundreds of students were attending the flagship course and there was considerable interest in research. In response, an expansion of the program began and in the fall of 1994 the NPS Academic Council approved the addition of a sequence of new courses to the Computer Science curriculum: Secure Management of Systems; Network Security; Secure Systems; Security Policies, Models and Formal Methods; and Database Security. Combined with the NPS thesis requirement for all Masters-level students, the academic program provides graduates with the knowledge needed to manage and contribute to engineering teams tasked not only to design and build secure systems, but also to configure and maintain them. The strong science and engineering education of NPS CISR graduates helps them to address new problems and to distinguish “snake oil” and marketing hyperbole from credible security solutions.

NPS CISR serves DoD in eight primary areas:

Curriculum. The explosive growth of information systems has resulted in rapidly changing technologies and challenges in computer security. Curriculum development ensures a timely, coherent and comprehensive program in INFOSEC foundations and technology.

Laboratory. Development of the Computer Security Laboratory has supported all aspects of the NPS CISR effort. Because major commercial vendors do not build systems and software that can be relied upon to protect sensitive information, security architectures including a mixture of both popular products and those specialized for computer security are found in the laboratory. The NPS CISR laboratory has supported over 250 students in work on assignments and laboratory exercises during the past year. Used for a variety of research projects, the facilities enable participants to explore the hardware and software available to solve current computer security problems and to consider potential future architectures and technologies.

Faculty. NPS CISR has an active program to increase the sophistication of faculty in INFOSEC concepts and to involve interested faculty members in leading-edge INFOSEC research problems. The results have been not only an increased appreciation of the foundations of computer security but a heightened understanding of the need to consider security throughout the entire process of design and development of systems. Several successful research efforts have been launched or assisted as a result of the faculty development effort.

Visiting Professors. The Visiting Professor program brings computer and network security experts to NPS to

-- *continued on page 36*

CISR, *continued from page 5*

participate in courses and engage in collaborative research. The program helps accelerate technology transfer between academe and industry. Visiting professors participate in NPS CISR programs for periods from a month to a year.

Invited Lectures. The Invited Lecture Series injects commercial and military relevance into the NPS CISR activities. Leading experts in the field of computer science and INFOSEC from government, academe, and industry address the students, staff, and faculty. A few of the invited lecturers are: Dr. Roger Schell, Novell; Dr. Paul Karger, IBM; Dr. John McLean, Naval Research Laboratory; Dr. Thomas Berson, Anagram Laboratories; and Terry Benzel, Trusted Information Systems.

Academic Outreach. Academic outreach permits other, non-CISR academic institutions to benefit from the education and research developments at NPS. For the past two years NPS CISR has sponsored the Workshop on Education in Computer Security (WECS). Attended by participants from Europe and North America, WECS has provided educators with an opportunity to hear from government and industry, and discuss educational requirements, develop strategies for academic programs, and share pedagogical material. NPS CISR has prepared material for dissemination to those needing a jump-start into computer security teaching. A CD with complete class notes has been very popular as is the NPS CISR web site at http://cisr.nps.navy.mil/. The invited lecture series is video taped for later distribution.

Graduates. An effort to insure that NPS graduates involved in NPS CISR courses and research are recognized so that their expertise can be applied to the wide variety of INFOSEC challenges in DoD and the U.S. Government is best achieved by making appropriate organizations aware of the growing talent pool of computer security savvy students and graduates emerging from NPS CISR. Currently, the expertise of our students is being used at DISA, Fleet Information Warfare Center, SPAWAR, NSA, and many other commands.

Research. DoD has long been involved in the development of secure systems and NPS was active in computer security research as early as 1978, well before the topic became highly visible.The rapid evolution of networking within DoD and DoN has lead to the connection of most computer systems to LANs and the use of WANs for data transport. Security mechanisms have lagged efforts at interconnection and now leave these systems vulnerable to exploitation by adversaries attempting either to compromise information within the systems or deny access to the systems themselves. Security for systems that must process both classified and unclassified information is an underlying theme of the diverse NPS CISR research.

Students from many NPS curricula including: Information Technology Management, C4I, and Information Warfare, join those in Computer Science to conduct thesis research with NPS CISR faculty. Research has included the following information assurance and computer and network security topics: protocols and mechanisms to improve the security of Internet Protocol (IP) over Asynchronous Transfer Mode (ATM) networks; utilization of system mechanisms to provide security for applications in heterogeneous distributed environments; issues associated with

-- continued on page 37

RADIO FREQUENCY PLANNER, *continued from page 35*

The NPS Ph.D. dissertation of **CDR Gus Lott**, currently an Assistant Professor in the Department of Electrical and Computer Engineering, played an important role in the development of the RFMP. The heart of this new view into the RF space is the “Lott Plot.” Developed by CDR Lott, this visualization technique displays the joint signal and noise probability density. The user can manipulate physical parameters to see how the “probabilities” vary. After leaving NPS and serving as Chief Engineer of the Naval Information Warfare Activity, CDR Lott took his research into application development.

RFMP is making the next step with the development of a more generalized Electromagnetic Propagation Server (EMPS). Under this concept, a large host of propagation models provides service on the GCCS LAN for any user application. Again, the “Lott Plot” becomes the fundamental method for determining the decision-maker’s metric.

RFMP is available at NPS on a local TAC-4 HP UNIX workstation. For more information on RFMP, persons interested can see a demonstration at: http://www.arlut.utexas.edu/~rfmpwww/public_page/rfmp_home/.

CISR, *continued from page 36*

security and quality of service; examination of signature identification mechanisms for malicious software, such as viruses; network intrusion detection and response; high assurance techniques for the creation of execution domains; utilization of existing high assurance multilevel products in near-term architectures to achieve operational multilevel secure network solutions; analysis of products which could be used to enhance the protection of sensitive but unclassified information; and the development of DoD-relevant strategies for the analysis of software security products.

A problem for DoD systems includes not only the provision of control of access to and movement of data based on fixed sensitivity levels, but the preservation of compatibility with commercial-off-the-shelf (COTS) application software as well. When compatibility with COTS applications takes precedence, often each access class is relegated to an independent system-high enclave and sharing is achieved through: manual, “sneaker-net” techniques; automated guards for which no notion of sufficiency or completeness with respect to security policy enforcement can be demonstrated; or replication systems relying on physical separation. All can be costly in terms of space, equipment and administration. NPS CISR faculty, staff, and students are constructing a COTS-driven Local Area Network that will provide multilevel secure (MLS) services to users while permitting them to employ standard office productivity tools on standard workstations. The ongoing development centers on the provision of multilevel mail and messaging to the desktop.

Increasingly, ATM is being used in DoN networks and techniques to move IP traffic over ATM networks are being explored. Unfortunately, current proposed standards for the transport of IP packets over ATM networks are silent regarding packet security. Faculty and students are examining techniques to provide security for IP traffic in ATM networks. Two areas are being investigated: the design of a network access controller to support IP over ATM seamlessly while preventing the flow of unauthorized information from a secure enclave; and investigation of a security protocol and mechanism for fast IP packet forwarding at the data link layer.

Defense in Depth, the DoN approach to network security, will use network intrusion detection tools. The concept of an intrusion detection system based upon the use of autonomous agents has been proposed. Deployable in heterogeneous environments, agents would be configurable to their execution environment.

Participating in a project that has as a goal quality of service for end-to-end applications in a highly dynamic environment, NPS CISR faculty, staff, and students are examining techniques to provide security for core services as well as for applications. A layered application architecture has been developed that builds upon notions of least privilege and separation of duty. A second aspect of this work is to treat processing for security as a factor in overall quality of service delivered by the system. This work will help to parameterize security choices.

NPS CISR research is funded by the National Security Agency, the Naval Security Group, SPAWAR, and DARPA. The NPS CISR members include Assistant Professor **Cynthia Irvine**, Associate Professor **Bert Lundy**, Visiting Associate Professor **Bret Michael**, Associate Professor **Neil Rowe**, Associate Professor **Tim Shimeall**, Associate Professor **Dennis Volpano**, Lecturer **Daniel Warren**, and Assistant Professor **Geoff Xie** of the Department of Computer Science, and Professor **Hal Fredricksen**, of the Department of Mathematics.

MBCORC, *continued from page 18*

programmatic relationship. “Crescent” evokes the arc of the Monterey Bay rim as well as the growing and emerging character of the institutions.

Initial signatories to the agreement were the California State University, Monterey Bay, Monterey Bay Aquarium, Monterey Bay Aquarium Research Institute, Monterey Institute of International Studies, Moss Landing Laboratories, University of California, Santa Cruz, University of California, MBEST Center, and the Naval Postgraduate School. Future parties to the agreement, in official or ex-officio status, include NOAA, the Naval Research Laboratory-Monterey, Fleet Numerical Meteorology and Oceanography Center, and the Monterey Advanced Technology Education Center of Monterey Peninsula College.